REMARKS

This Preliminary Amendment and the accompanying Request for Continued Examination ("RCE") are being filed in response to the Final Office Action mailed August 4, 2005. A check for $790.00 to cover the RCE filing fee payment is included with this Amendment. If necessary, please charge any other fees for entry of this Amendment and RCE to our deposit account no. 03-3415.

Claims 7 and 20 have been cancelled. Claims 1, 6, 8, 14, 14, 19, 21 and 26-30 have been amended.

The Examiner has rejected applicant's claims 1, 3-14 and 16-20 and maintained the rejections from the previous Office Action. In particular, claims 1, 3, 6-16 and 19-30 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Anderson (U.S. Publication No. 2002/0052923). Applicant notes that in the previous Office Action dated March 29, 2005, the Examiner has mentioned, on pages 4 and 5, a second reference ("Beck") in combination with the Anderson reference. However, the Examiner has not supplied a patent or publication number and has not listed such reference on Form PTO-892 (Notice of References Cited) in either the previous Office Action of March 29, 2005 or the present Office Action. In view of the above, and because the Examiner has previously listed grounds for rejection based on "Anderson in view of Beck" under the heading of claim rejections under 35 U.S.C. § 102(e), applicant has treated such rejections to be based on Anderson alone under 35 U.S.C. § 102(e). Applicant's claims 4 and 17 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Anderson in view of McArdle et al. (U.S. Patent No. 6,442,686), and claims 5 and 18 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Anderson in view of Baxter

Jr. (U.S. Patent No. 6,385,306). With respect to applicant's claims, as amended, the Examiner's rejections are respectfully traversed.

Applicant's independent claims 1, 13, 14 and 26-30 have been amended to better define applicant's invention. Applicant's claim 1 has now been amended to recite a communication system having a server for providing a Web E-mail service to a client, wherein said server comprises management means for managing a key for decrypting an encrypted E-mail, web encryption communication means for establishing a Web encryption communication with a client, and communicating with the client by the established Web encryption communication, authentication means for executing authentication of the use allowance of the managed key to the client when the client requests to decrypt the encrypted E-mail while the server communicates with the client by the established Web encryption communication, decrypting means for decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated by the authentication means, and transmission control means for controlling to transmit the E-mail decrypted by the decrypting means to the client through the established Web encryption communication. Applicant's independent claims 13, 14 and 26-30 have been similarly amended.

Applicant's amended independent claim 13 further recites the client comprising request means for requesting to decrypt the encrypted E-mail while the Web encryption communication is established between the server and the client, authentication information sending means for sending the authentication information to the authentication means, and receiving means for receiving the decrypted E-mail transmitted by the transmission control means through the established Web encryption communication. Applicant's independent claims 26, 28 and 30 have been similarly amended.

The constructions recited in applicant's amended independent claims 1, 13, 14 and 26-30 are not taught or suggested by the cited art of record. In particular, the Examiner has argued in the previous Office Action dated March 29, 2005 that Anderson discloses encryption communication means for establishing and communicating the Web encryption communication when communicating with the client through the Web (Anderson: see for example, Para [0019] Line 6-10: to deliver the Email across the network such as internet URL (HTTP) through various nodes and links until it reaches the recipient users), and transmission means for transmitting the use allowance by the authentication means and the E-mail decrypted by the decrypting means to the client after the Web encryption communication is established by the encryption communication means (Anderson: see, for example, Para [0006] Line 9-15 and Para [0019] Line 1-10).

Applicant has reviewed the passages of Anderson cited by the Examiner and believes that there is no teaching or suggestion in the Anderson reference of establishing a Web encryption communication with the client and communicating with the client by the established Web encryption communication. Specifically, paragraph [0019] of Anderson teaches that a message indicator sent to the user may include a link, such as a URL, which allows manual access to the message by the client. This paragraph merely teaches that a message can be accessed by the client over the Internet and makes no mention of any Web encryption communication or of communicating with the client by the established Web encryption communication.

Applicant's review of the remaining portions of the Anderson reference confirms that the Anderson reference is completely silent as to establishing the Web encryption communication with the client and communicating with the client by the established Web

encryption communication. Specifically, Anderson discloses that a message sender can encrypt a message with a public encryption key of a server (Step 320 of FIG. 3, Paragraph [0036]) and that a message distributor then decrypts the message with a server's private key (Step 515 of FIG. 5; Paragraph [0038]) and stores the unencrypted message (Step 533 of FIG. 5; Paragraph [0038]). When the message that was originally encrypted is transmitted to the client, i.e., the response is "Yes" in Step 540 of FIG. 5, the stored unencrypted message is re-encrypted with the public key of each client computer and the encrypted message is then transmitted to the client computer (Step 550 of FIG. 5; Paragraphs [0039-0040]), and the client computer decrypts the received message with a private key of the client computer (Paragraph [0044], lines 5-9). Thus, in Anderson, a message is encrypted with a public key of the client before it is transmitted and then decrypted by the client using its private key, and there is no mention in Anderson of a Web encryption communication being established with the client computer or of communicating with the client by the established Web encryption communication. Accordingly, applicant's independent claims 1, 13, 14 and 26-30, each of which recites such features, patentably distinguish over the Anderson reference. Further, there is nothing taught or suggested in the McArdle and the Baxter patents that would change this conclusion.

Moreover, the cited references fail to teach or suggest authentication of the use allowance of the managed key to the client when the client requests to decrypt the encrypted E-mail while the server communicates with the client by the established Web encryption communication, and controlling transmission of the email decrypted by the decrypting means to the client through the established Web encryption communication. First, as discussed herein above, the Anderson reference fails to teach or suggest establishing a Web encryption communication with the client and communication with the client thereby. In addition,

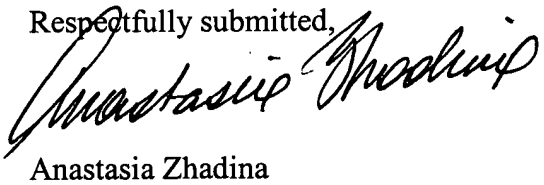
Anderson teaches in paragraphs [0040] and [0044] that the unencrypted message stored by the message distributor is encrypted before being transmitted to the client and that the decryption is performed by the client after the encrypted message is received by the client. Thus, in Anderson, the message that is transmitted to the client is encrypted, not decrypted, and the decryption of the message is performed on the client-side after the transmission. Therefore, there is clearly no teaching or suggestion in Anderson as to executing authentication when decryption of the email is requested while the serve communicates with the client by the established Web encryption communication, and controlling to transmit a decrypted email to the client through the established Web encryption communication. Applicant's independent claims 1, 13, 14 and 26-30, each of which recites these features, thus patentably distinguish over the Anderson reference. The cited McArdle, et al. and Baxter, Jr. patents add nothing to change this conclusion.

In view of the above, applicant's independent claims 1, 13, 14 and 26-30, and their respective dependent claims, thus patentably distinguish over the cited art of record, and are therefore submitted as patentable. Reconsideration of these claims is thus respectfully requested.

If the Examiner believes that an interview would expedite consideration of this Amendment or of the application, a request is made that the Examiner telephone applicant's counsel at (212) 790-9286.

Dated: November 4, 2005

Respectfully submitted,



COWAN, LIEBOWITZ & LATMAN, P. C.
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200

Anastasia Zhadina
Reg. No. 48,544
Attorney of Record